Remarks

The above Amendments and these Remarks are in reply to the Office Action mailed January 7, 2009.

I. Summary of Examiner's Rejections

Prior to the Office Action mailed January 7, 2009, Claims 1-28, 45-51 and 60-69 were pending in the Application. In the Office Action, Claims 1, 3-9, 11-15, 17-23, 25-28, 45-51, 60-61, 63-65 and 69 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Heiner (U.S. Patent No. 6,112,227, hereinafter Heiner) and Kirsch (U.S. Patent No. 6,546,416, hereinafter Kirsch), in further view of applicant's admitted prior art (hereinafter AAPA), and Espinosa et al. (U.S. Publication No. 2007/0204043, hereinafter Espinosa). Claims 2, 10, 16, 24, 62, 66, and 69 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Heiner, Kirsch, Espinosa and AAPA, as applied to claims 1, 7, 15, and 21, in view of what is well known in the art.

II. Summary of Applicants' Amendment

The present Response amends Claims 1, 7, 15, 21 and 45, cancels Claim 51, and adds new Claim 70, leaving for the Examiner's present consideration Claims 1-28, 45-50 and 60-70. Reconsideration of the Application, as amended, is respectfully requested. Applicants respectfully reserve the right to prosecute any originally presented or canceled claims in a continuing or future application.

III. Claim Rejections under 35 U.S.C. § 103(a)

In the Office Action mailed January 7, 2009, Claims 1, 3-9, 11-15, 17-23, 25-28, 45-51, 60-61, 63-65 and 69 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Heiner (U.S. Patent No. 6,112,227, hereinafter Heiner) and Kirsch (U.S. Patent No. 6,546,416, hereinafter Kirsch), in further view of applicant's admitted prior art (hereinafter AAPA), and Espinosa et al. (U.S. Publication No. 2007/0204043, hereinafter Espinosa). Claims 2, 10, 16, 24, 62, 66, and 69 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Heiner, Kirsch, Espinosa and AAPA, as applied to claims 1, 7, 15, and 21, in view of what is well known in the art.

Claim 1

Claim 1 has been amended to more clearly define the embodiment therein. As amended, Claim 1 defines:

> *1. A method for modifying mail filters associated with a user of a mail system, the method comprising:*
>
> *receiving a subscription request from a recipient to a sender, the subscription request including user information, wherein the subscription request is received as part of a web browser interaction before sending electronic mail between the sender and the recipient and wherein the subscription request is initiated by the recipient;*
>
> *generating a petition by the sender based on the user information, the petition comprising a request for the sender to be added to a list of approved mail senders, the list associated with the user, wherein inside the petition the sender specifies a set of methods that the sender will use to identify itself in a future time when the sender sends the electronic mail to the recipient;*
>
> *transmitting a token containing the petition from the sender to the recipient as a result of the subscription request and storing said token at a computing device where the recipient resides, wherein the petition is transmitted during said web browser interaction before sending electronic mail between the sender and the recipient;*
>
> *receiving a login request from the user to the mail system;*
>
> *checking for the token containing the petition in the computing device where said recipient resides;*
>
> *processing said token containing the petition if the token is found on the computing device where the recipient resides and modifying the mail filters associated with the user by adding the sender to the list of approved mail senders as specified in the petition; and*
>
> *transmitting an electronic mail message from the sender to the recipient, wherein the set of methods specified by the sender in the petition are employed by the recipient to verify the sender's identity that transmitted the electronic mail message.*

Claim 1 has been amended to more clearly define certain features therein. Specifically, amended Claim 1 defines that inside the petition, the sender specifies a set of methods that the sender will use to identify itself in a future time when the sender sends the electronic mail to the recipient. This petition is created during a web browser interaction, when a future email recipient submits a subscription request to the sender. At that time, the petition is sent as a token to the recipient, before any emails need to be exchanged between the sender and the recipient.

When the recipient receives the token, it stores it at the recipient's computer. Subsequently, when the recipient user logs into the email system, the petition processor checks the recipient's computer for the token containing the petition. If the token is found, the petition processor will process the petition and, if it is acceptable, the mail filters on the recipient will be modified to add the sender.

At a future time, when the sender transmits an email to the recipient, the set of methods previously specified by the sender in the petition are then employed by the recipient to verify the sender's identity. For example, the sender may have specified a "header-password" type method in the petition, wherein the sender will always include a header password in its email messages to the recipient. As another example, the sender may have specified a public key in the petition, which can be used to decrypt a digital signature accompanying the sender's email to the recipient.

An advantage of this type of functionality is that the sender and recipient can avoid legitimate email which has been sent by a software program from getting caught in the junk-mail filters of the recipient mail system, all without having to manually keep track of their whitelists (e.g. see new Claim 70). In addition, the system maintains security because the sender's specified identification methods in the petition prevent other senders from impersonating the identity of the sender.

Heiner teaches a method for preventing the delivery of unwanted email messages. As disclosed in Heiner, "an original electronic message is first received from a source client at a destination server. Next, a reply electronic message is sent from the destination server to the source client requesting the source client to complete a registration process…." (Heiner, Abstract). The email is only delivered when the source client completes the registration process. If "the original message is junk email produced by a robotic delivery program, the destination SMTP server will never receive a response to its reply message because the source client e-mail address does not exist." (Heiner, col. 3, lines 39-55).

Kirsch teaches a similar challenge/response mechanism to Heiner. This mechanism is also designed for blocking delivery of bulk electronic mail. As disclosed in Kirsch, the system prepares "in response to the receipt of a predetermined e-mail message fro an unverified source address, a signature key… This email message, including the data key is then issued to the unverified source address. The computer system then operates to detect whether an e-mail message, responsive to the challenge e-mail message is received and whether this response e-mail message includes a response key…" (Kirsch, col. 3, lines 43-67).

Espinosa also teaches a system for rejecting unauthorized or spam e-mail messages. As disclosed therein, the system rejects "junk mail by using an access code that the sender inserts anywhere in the … e-mail message, and only those e-mail messages containing a valid access code … are delivered." (Espinosa, Abstract) The access code has either been "previously defined by the recipient… or it can be dynamically generated…" Espinosa, par. [0015]).

In addition, Espinosa describes an improvement to this method to obtain the access code, where "when an e-mail is sent to the e-mail owner without the access code, … the message is not delivered to the inbox but returned to the sender with instructions to access an Internet page that lets the sender obtain the code only if he/she knows personal key information of the owner." (Espinosa, par. [0015]).

From the above description, it appears that all of the cited references (Heiner, Kirsch and Espinosa) appear to describe ways to block unwanted email from automated "bulk" senders. However, Applicant respectfully submits that the cited references fail to render obvious the features of Claim 1, as amended.

In the Office Action, it was agreed that Heiner does not disclose a token containing the petition. It was proposed however, that "Kirsch discloses generating and transmitting a digital signature containing a valid petition to add a sender to an approved sender list (column 3, lines 43-57, a digital signature (token) is transmitted to verify a sender." (Office Action, page 4).

Applicant respectfully disagrees. The cited portion of Kirsch discloses a signature key that is sent as a challenge in response to an email received. This is not the same as a petition that is transmitted during said web browser interaction before sending electronic mail between the sender and the recipient, as defined in Claim 1. It is clearly evident from the disclosure in Kirsch, that the signature key is sent after receiving an email (*see* "preparing, in response to the receipt of a predetermined e-mail message from an unverified source, a signature data key…" Kirsch col. 3, lines 46-48). Because the petition of Claim 1 is sent before exchanging emails, it can avoid all junk mail filters and blockers of the recipient, which would normally block transmissions from the sender.

In the same way, Heiner and Espinosa also fail to disclose sending any petition that is transmitted before sending electronic email. For example, in Heiner "an original electronic mail message is first received from a source client… Next, a reply electronic message is sent…” (Heiner, Abstract). Thus, Heiner only performs functions after receiving an email message and does not send any petitions before that. Similarly, Espinosa performs all its functions after receiving an email (*see* “When an e-mail is sent to the e-mail owner, without the access code… the message is not delivered to the inbox but returned to the sender with instructions to access an Internet page.” (Espinosa, par. [0015]).

In addition, the cited references fail to disclose a petition token sent to the recipient, wherein inside the petition the sender specifies a set of methods that the sender will use to identify itself in a future time when the sender sends the electronic mail to the recipient, as defined in amended Claim 1. This type of petition is not described in any of the cited references. For example, Kirsch describes a signature data key that is issued as a response to an email message from an unverified source (col. 3, lines 45-48). However, this signature key is different from a petition. Inside the petition of Claim 1, the sender specifies a set of methods that the sender will use to identify itself in a future time when the sender sends the electronic mail to the recipient. Thus, the sender uses the petition to specify its own identification methods that it will use in the future to identify itself. In contrast, the signature key disclosed in Kirsch, is issued by the recipient. It is used to challenge (ask) the sender for some predetermined information. As such, there is no way for the sender to specify its own preferable methods of identifying itself in the future to the recipient. Rather, the sender must answer a challenge email.

In the same way, the cited references fail to disclose that at the time of sending the email message, the set of methods which were previously specified by the sender in the petition are employed by the recipient to verify the sender’s identity that transmitted the electronic mail message, as defined in Claim 1.

In view of the above comments and amendments, Applicants respectfully submit that Claim 1, as amended, is neither anticipated by, nor obvious in view of the cited references, and reconsideration thereof is respectfully requested.

Claims 7, 15, 21 and 45

Claims 7, 15, 21 and 45 while independently patentable, recite limitations that, similarly to those described above with respect to claim 1 are not taught, suggested nor otherwise rendered obvious by the cited references. Reconsideration thereof is respectfully requested.

Claims 2-6, 8-14, 16-20, 22-28, 46-51 and 60-67

Claims 2-6, 8-14, 16-20, 22-28, 46-51 and 60-67 are not addressed separately, but it is respectfully submitted that these claims are allowable as depending from an allowable independent claim, and further in view of the comments provided above. Applicants respectfully submit that Claims 2-6, 8-14, 16-20, 22-28, 46-51 and 60-67 are similarly neither anticipated by, nor obvious in view of the cited references, and reconsideration thereof is respectfully requested.

It is also submitted that these claims also add their own limitations which render them patentable in their own right. Applicants respectfully reserve the right to argue these limitations should it become necessary in the future.

VI. <u>New Claim</u>

The present Response adds new dependent Claim 70. New Claim 70 is fully supported by the Specification as originally filed and no new matter is being added.

In addition to the features discussed above, Claim 70 requires that the petition, once processed by the recipient, causes the electronic mail message generated by an automated mail program of the sender to bypass the recipient's email filters. This feature is entirely different from what is disclosed in the cited references. In fact, Heiner, Kirsch and Espinosa actually appear to teach away from this feature because their intended purpose is to block email from automated mail programs. For example, the purpose of Kirsch appears to be "to enable blocking of e-mail from bulk e-mail sources." (col. 3, lines 44-46). Similarly, in Heiner "if the original message is junk e-mail produced by a robotic delivery program, the destination SMTP server will never receive a response to its reply message…" (col. 3, lines 50-55). In the same way, Espinosa requires a sender "to respond to personal questions about the e-mail owner…" (Espinosa, Abstract) which appears to be to discriminate against automated programs that generate email. In contrast, Claim 70 specifically requires that the petition causes the email generated by the automated mail program to bypass the recipient's email filters. As such, Claim 70 is also not rendered obvious by the cited references.

VII. Conclusion

In view of the above amendments and remarks, it is respectfully submitted that all of the claims now pending in the subject patent application should be allowable, and reconsideration thereof is respectfully requested. The Examiner is respectfully requested to telephone the undersigned if he can assist in any way in expediting issuance of a patent.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 06-1325 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: May 7, 2009

By: /Justas Geringson/
Justas Geringson
Reg. No. 57,033

Customer No.: 23910
FLIESLER MEYER LLP
650 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 362-3800
Fax: (415) 362-2928